FortiAnalyzer
Upgrade Guide

FortiAnalyzer Upgrade Guide

May 13, 2013

05-502-200816-20130513

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2013-05-13	Initial release.

FortiAnalyzer Firmware

This document provides an overview of FortiAnalyzer firmware and highlights general information you should be aware of prior to upgrading your FortiAnalyzer device. This guide is intended to supplement the *FortiAnalyzer Release Notes* documentation.

The following topics are included in this section:

- Best practices
- Firmware image naming convention
- FortiAnalyzer VM firmware
- Build numbers
- Firmware upgrade and support information

Best practices

Before any firmware upgrade complete the following:

- Download the FortiAnalyzer firmware image and Release Notes document from the Customer Service & Support website. Review the Release Notes including special notices, upgrade information, product integration and support, resolved and known issues.
- Prepare your FortiAnalyzer for upgrade and ensure your log devices are running the appropriate firmware versions as documented in the firmware Release Notes.
- Backup your configuration file and save this configuration file to your local computer. The device configuration file is saved with a .dat extension.

In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

- Plan a maintenance window to complete the firmware upgrade. If possible, you may want to set up a test environment to ensure that the upgrade does not negatively impact your network or log devices.
- Once the upgrade is complete, test your FortiAnalyzer device to ensure that the upgrade was successful and that all log devices are listed.

Firmware best practice: Stay current on patch releases for your current major release. Only upgrade to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the *FortiAnalyzer Release Notes* or contact Fortinet Technical Support.

Firmware image naming convention

FortiAnalyzer firmware images on the Customer Service & Support site FTP directory are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model. For example, the FAZ_200D-v500-build0151-FORTINET.out image found in the v5.0 Patch Release 2 directory is specific to the FortiAnalyzer 200D device model and the FLG_1000C-v400-build0705-FORTINET.out image found v4.0 MR3 Patch Release 7 directory is specific to the FortiAnalyzer 1000C device model.

Figure 1 shows the version 5.0 Patch Release 2 FTP directory and highlights the FortiAnalyzer v5.0 Patch Release 2 firmware image for the FortiAnalyzer 200D and the location of the *FortiAnalyzer v5.0 Patch Release 2 Release Notes*.

You can also download the Fortinet-FortiManager-FortiAnalyzer MIB file in this directory. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 directory.

Figure 1: v5.0 Patch Release 2 FTP directory

FTP directory /FortiAnalyzer/v5.00/5.0/5.0.2/ at support.fortinet.com

To view this FTP site in Windows Explorer: press Alt, click **View**, and then click **Open FTP Site in Windows Explorer**.

Up to higher level directory

03/29/2013 06:07PM	28,787,144	FAZ_1000B-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,868,555	FAZ_1000C-v500-build0151-FORTINET.out
03/29/2013 06:07PM	27,273,547	FAZ_100C-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,777,721	FAZ_2000A-v500-build0151-FORTINET.out
03/29/2013 06:07PM	29,129,611	FAZ_2000B-v500-build0151-FORTINET.out
03/29/2013 06:07PM	29,290,329	FAZ_200D-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,631,919	FAZ_4000A-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,940,936	FAZ_4000B-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,265,176	FAZ_400B-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,574,042	FAZ_400C-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,760,129	FAZ_VM32-v500-build0151-FORTINET.out
03/29/2013 06:07PM	28,600,486	FAZ_VM32-v500-build0151-FORTINET.out.ovf.zip
03/29/2013 06:07PM	29,307,131	FAZ_VM64-v500-build0151-FORTINET.out
03/29/2013 06:07PM	29,141,319	FAZ_VM64-v500-build0151-FORTINET.out.ovf.zip
04/24/2013 09:54PM	614,913	FortiAnalyzer-v5.0-Patch-Release-2-Release-Notes.pdf
03/29/2013 06:07PM	Directory	MIB

FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for 32-bit and 64-bit systems in two formats:

- FAZ_VMxx-v500-build0xxx-FORTINET.out: Download either the 32-bit or 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- FAZ_VMxx-v500-build0xxx-FORTINET.out.ovf.zip: Download either the 32-bit or 64-bit package for new FortiAnalyzer VM installations. The package contains a deployable Open Virtualization Format (OVF) virtual machine package for VMware ESX/ESXi installations and the faz.vmdk and datadrive.vmdk virtual machine disk format files.

For more information see the FortiAnalyzer product datasheet available on the Fortinet web site, http://www.fortinet.com/products/fortianalyzer/virtualappliances.html.

Build numbers

FortiAnalyzer firmware images are generally documented as a three-digit build number. New FortiAnalyzer models may be released on a special branch based off of the regular FortiAnalyzer firmware release. As such, the build number found in the *System Settings* > *General* > *Dashboard, System Information* widget and the output from the `get system status` CLI command displays this four-digit special build number as the build number.

To confirm that you are running the proper build, the output from the `get system status` CLI command has a `Branch point:` field that displays the regular three-digit build number.

The following examples provide the output from the `get system status` CLI command for both a regular firmware release and a new model firmware release.

Example 1: Regular firmware release

```
Platform Type : FAZ2000A
Version : v5.0-build0151 130328 (GA Patch 2)
Serial Number : FLG-2K3F08000179
BIOS version : 04000001
Hostname : FortiAnalyzer-2000A
Max Number of Admin Domains : 2000
Max Number of Device Groups : 2000
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
Branch Point : 151
Release Version Information : (GA Patch 2)
Current Time : Wed Apr 24 14:20:53 PDT 2013
Daylight Time Saving : Yes
Time Zone : (GMT-8:00)Pacific Time(US&Canada)

Disk Usage : Free 1825.27GB, Total 1831.40GB
RAID Level: Raid-5
RAID Status: OK
RAID Size: 1862GB

Disk 1: OK Used 465GB
Disk 2: OK Used 465GB
Disk 3: OK Used 465GB
Disk 4: OK Used 465GB
Disk 5: OK Not-Used 465GB
Disk 6: OK Used 465GB
```

Example 2: New model firmware release

```
Platform Type : FAZ300D
Version : v5.0-build4015 130416 (GA)
Serial Number : FL300D3M13000001
BIOS version : 00010001
System Part-Number : P13424-01
Hostname : FAZ300D
Max Number of Admin Domains : 175
Max Number of Device Groups : 175
```

```
Admin Domain Configuration : Disabled
FIPS Mode : Disabled
Branch Point : 151
Release Version Information : (GA)
Current Time : Tue Apr 23 15:09:43 PDT 2013
Daylight Time Saving : Yes
Time Zone : (GMT-8:00)Pacific Time(US&Canada)

Disk Usage : Free 1831.09GB, Total 1833.78GB
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1953GB

Disk 1: OK Used 1953GB
Disk 2: OK Used 1953GB
```

Firmware upgrade and support information

The following table is for reference only. Review the applicable *FortiAnalyzer Releases Notes* prior to upgrading your FortiAnalyzer system.

The following table uses the naming convention '4.3.7', where the first digit reflects the version, the second digit reflects the major release, and the third digit reflects the patch release. For example, 4.3.7 is v4.0 MR3 Patch Release 7.

Table 1: FortiAnalyzer upgrade and support information

FortiAnalyzer Firmware Version	Build Number	Upgrade From	FortiOS Version Support
FortiAnalyzer 5.0			
5.0.3 Release Date: TBA			
FortiAnalyzer 5.0.3 is available for the following models:			
5.0.2 Release Date: 2013-03-28	0151 The FAZ-300D is released on special build 4018.	5.0.1	5.0.0 or later 4.3.2 or later 4.2.0 or later
FortiAnalyzer 5.0.2 is available for the following models: FAZ-100C, FAZ-200D, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
5.0.1 Release Date: 2012-11-21	0087	4.3.5 or later	5.0.0 or later 4.3.1 or later 4.2.0 or later
FortiAnalyzer 5.0.1 is available for the following models: FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-1000B, FAZ-1000C, FAZ-2000A, FAZ-2000B, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			

Table 1: FortiAnalyzer upgrade and support information (continued)

FortiAnalyzer Firmware Version	Build Number	Upgrade From	FortiOS Version Support
5.0.0 Release Date: 2012-11-01	0076	Note: This image was removed from the Customer Service & Support site. See the *Customer Support Bulletin* in the image directory.	
FortiAnalyzer 4.3			
4.3.7 Release Date: 2013-04-04	0705	4.3.5 or later 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.7 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.6 Release Date: 2012-12-05	0691	4.3.5 4.2.6	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.6 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.5 Release Date: 2012-07-24	0680	4.3.3 or later 4.2.5 or later	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.5 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. Note: There is no image available for the FAZ-200D.			
4.3.4 Release Date: 2012-07-18	0679	4.3.3 4.2.5 or later	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.4 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64. Note: There is no image available for the FAZ-200D.			
4.3.3 Release Date: 2012-05-15	0654 The FAZ-200D is released on special build 4010.	4.3.2 4.2.5 or later	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.3 is available for the following models: FAZ-100B, FAZ-100C, FAZ-200D, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.2 Release Date: 2012-03-19	0632 The FAZ-400C is released on special build 4006	4.3.1 4.2.5 or later	4.3.0 or later 4.2.0 or later
FortiAnalyzer 4.3.2 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-400C, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, FAZ-VM32, and FAZ-VM64.			
4.3.1 Release Date: 2011-10-06	0552	4.3.0 4.2.4 or later	4.3.0 or later 4.2.0 or later

Table 1: FortiAnalyzer upgrade and support information (continued)

FortiAnalyzer Firmware Version	Build Number	Upgrade From	FortiOS Version Support
FortiAnalyzer 4.3.1 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, FAZ-4000B, and FAZ-VM.			
4.3.0 Release Date: 2011-06-30	0513	4.2.4 or later	4.3.0 or later
FortiAnalyzer 4.3.0 is available for the following models: FAZ-100B, FAZ-100C, FAZ-400B, FAZ-800, FAZ-800B, FAZ-1000B, FAZ-1000C, FAZ-2000, FAZ-2000A, FAZ-2000B, FAZ-4000, FAZ-4000A, and FAZ-4000B. Note: There is no image available for the FAZ-VM.			
FortiAnalyzer 4.2 is no longer supported (EOS) as of April 07, 2013.			

Upon upgrading to FortiAnalyzer v5.0 Patch Release 1 or later, the system automatically begins converting the v4.0 MR3 logs, and inserts them into the SQL database. An icon appears at the top right corner after login to the Web-based Manager next to the logout and help buttons. This pops-up a small window displaying the progress. The time required depends on the size of the database.

Upgrading a FortiAnalyzer VM device from v4.0 MR3 Patch 5 (and above) to v5.0 Patch Release 1 or later is supported. The old VM license is converted into the new VM stackable license model. New VM installations running v5.0 Patch Release 1 or later can be deployed with the .ovf file and application of either an old v4.0 MR3 or new v5.0 license.

FortiGate and FortiCarrier devices are supported in FortiAnalyzer v5.0 Patch Release 1 or later, and are retained after upgrade. Other devices are not yet supported in FortiAnalyzer v5.0. For more information, see the *Firmware Release Notes*.

Upgrade Information

This section outlines the general firmware upgrade steps. The following topics are included in this section:

- General firmware upgrade steps
- Distributed upgrades
- Downgrading to previous versions

Please review the firmware Release Notes prior to upgrading. For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer Administration Guide* at http://docs.fortinet.com.

General firmware upgrade steps

The following table lists the general firmware upgrade steps.

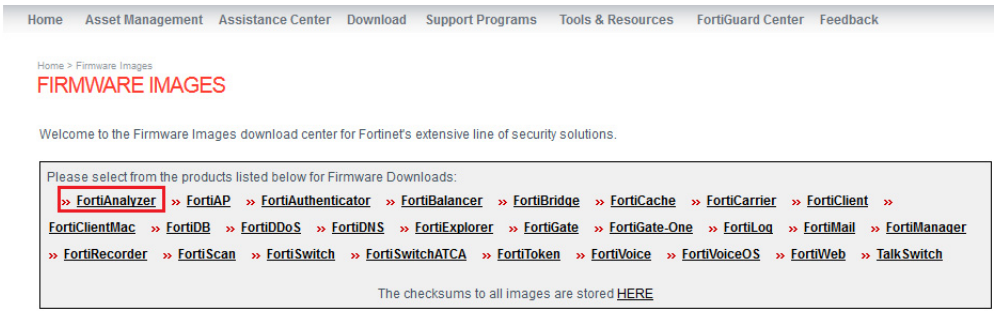
Table 2: Upgrade steps

Step 1	Prepare your FortiAnalyzer for upgrade.
Step 2	Backup your FortiAnalyzer system configuration. For FortiAnalyzer VM, take a *Snapshot* of the VM instance.
Step 3	Transfer the firmware image to your FortiAnalyzer device.
Step 4	Log into your FortiAnalyzer Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiAnalyzer for upgrade

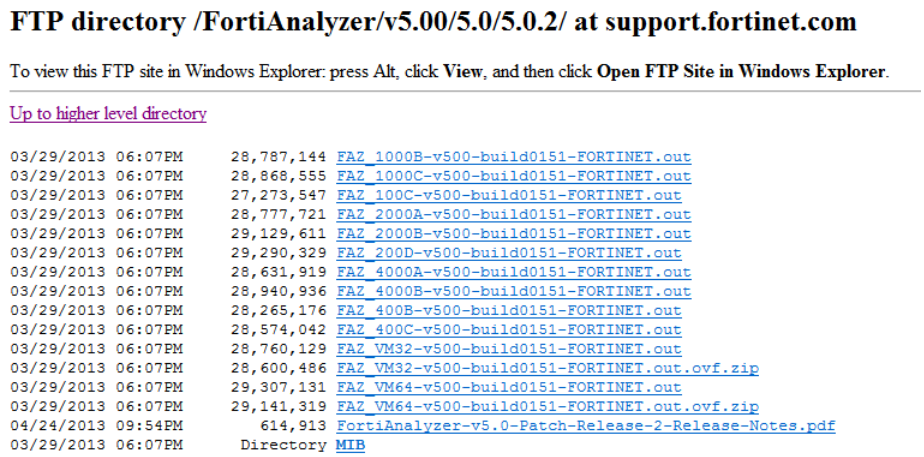
1. Make sure all log devices are running the supported firmware version as stated in the Release Notes.
2. Log in to the Customer Service & Support portal at https://support.fortinet.com.
3. In the *Download* section of the page, select *Firmware Images*, and select *FortiAnalyzer*

Figure 2: Firmware image page



4. Browse to the appropriate FTP directory to download the firmware image and Release Notes document.

Figure 3: Example FTP directory



FTP directory /FortiAnalyzer/v5.00/5.0/5.0.2/ at support.fortinet.com

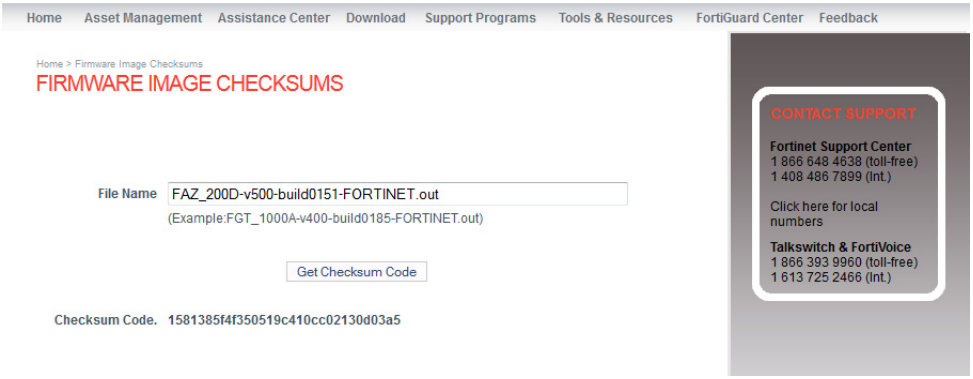
To view this FTP site in Windows Explorer: press Alt, click **View**, and then click **Open FTP Site in Windows Explorer**.

Up to higher level directory

```
03/29/2013 06:07PM     28,787,144 FAZ_1000B-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,868,555 FAZ_1000C-v500-build0151-FORTINET.out
03/29/2013 06:07PM     27,273,547 FAZ_100C-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,777,721 FAZ_2000A-v500-build0151-FORTINET.out
03/29/2013 06:07PM     29,129,611 FAZ_2000B-v500-build0151-FORTINET.out
03/29/2013 06:07PM     29,290,329 FAZ_200D-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,631,919 FAZ_4000A-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,940,936 FAZ_4000B-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,265,176 FAZ_400B-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,574,042 FAZ_400C-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,760,129 FAZ_VM32-v500-build0151-FORTINET.out
03/29/2013 06:07PM     28,600,486 FAZ_VM32-v500-build0151-FORTINET.out.ovf.zip
03/29/2013 06:07PM     29,307,131 FAZ_VM64-v500-build0151-FORTINET.out
03/29/2013 06:07PM     29,141,319 FAZ_VM64-v500-build0151-FORTINET.out.ovf.zip
04/24/2013 09:54PM        614,913 FortiAnalyzer-v5.0-Patch-Release-2-Release-Notes.pdf
03/29/2013 06:07PM      Directory MIB
```

5. To verify the integrity of the download, go back to the *Download* section of the login page, then select the *Firmware Image Checksums* link.

Figure 4: Firmware image checksums page

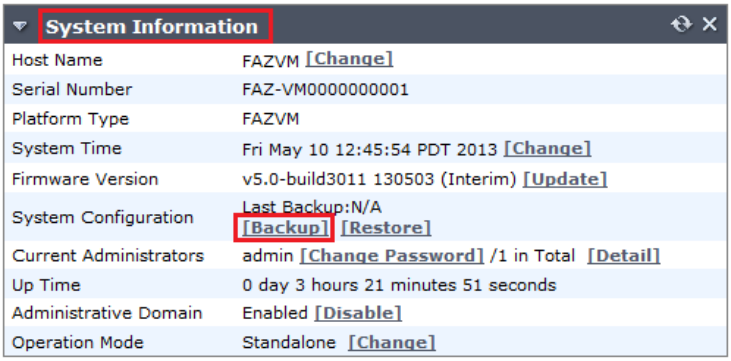


6. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Back up your FortiAnalyzer configuration

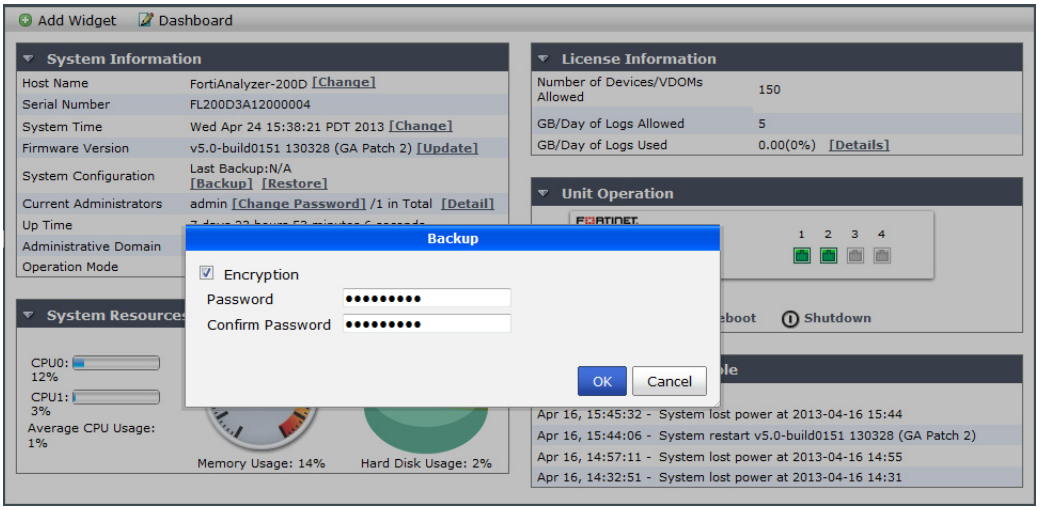
1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, under *System Configuration*, select *Backup*.

Figure 5: System information widget



The *Backup* dialog box opens.

Figure 6: Backup dialog box



3. Select the checkbox to encrypt the backup file and enter a password.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiAnalyzer device.

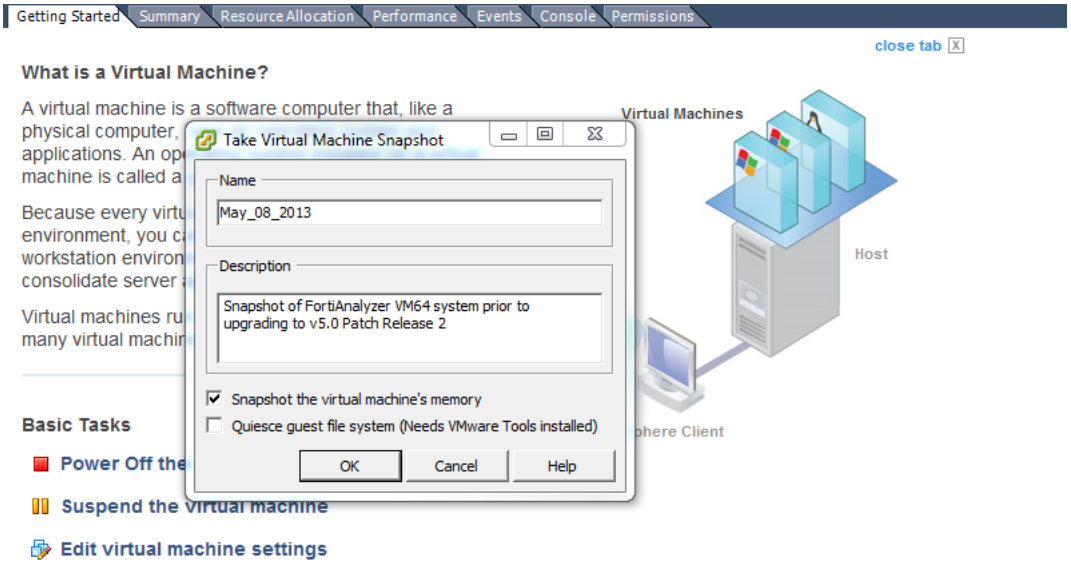
4. Select *OK* and save the backup file on your local computer.

Optionally, you can backup the configuration file to a FTP or SCP server using the following CLI command:

```
execute backup all-settings <ftp | scp> <ip> <path/filename save to
    the server> <username on server> < password>
```

5. In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

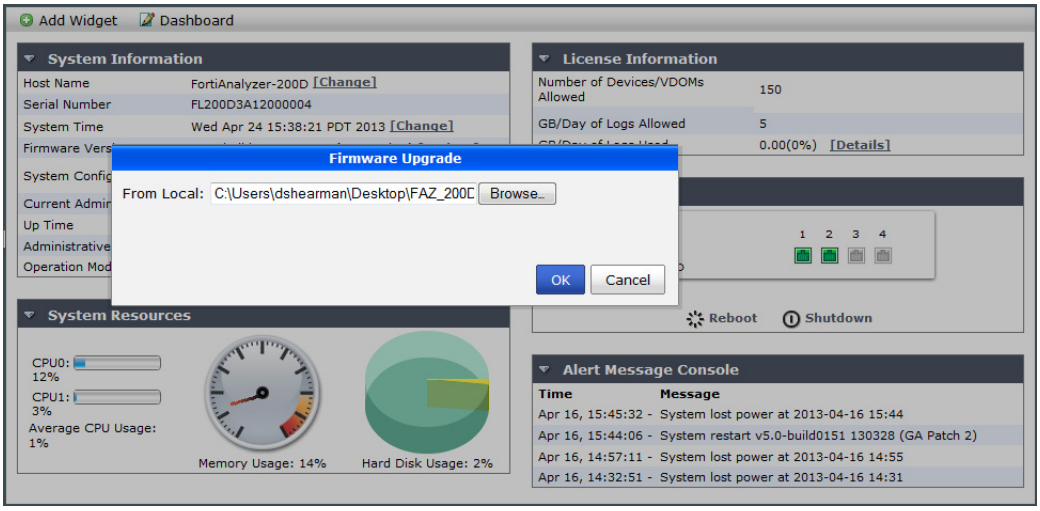
Figure 7: Snapshot of FortiAnalyzer VM



Step 3: Transfer the firmware image to your FortiAnalyzer device

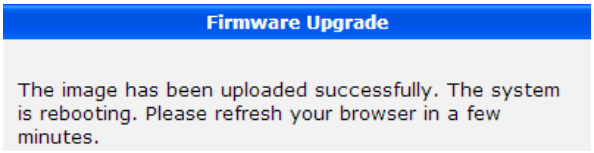
1. Go to *System Settings* > *General* > *Dashboard*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.
   The *Firmware Upgrade* dialog box opens.

Figure 8: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware package (`.out` file) that you downloaded from the Customer Service & Support web site and select *Open*.
4. Select *OK*. *Your* FortiAnalyzer will upload the firmware image and you will receive the following message.

Figure 9: Firmware upgrade successful dialog box



Optionally, you can upgrade firmware stored on an FTP or FTP server using the following CLI command:

```
execute restore image <ftp | tftp> <file path to server> <ip of
    server> <username on server> <password>
```

Step 4: Verify the upgrade

1. Refresh the browser page and log back into the device.
2. Launch the *Device Manager* module and make sure that all formerly added log devices are still listed.
3. Launch the other functional modules and make sure they work properly.

Distributed upgrades

For Collector/Analyzer architecture upgrades, Fortinet recommends upgrading the Analyzer first.

Upgrading the Collector first could impact the Analyzer's performance.

Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous FortiAnalyzer firmware release via the Web-based Manager or CLI. FortiAnalyzer. A system reset is required after the firmware downgrading process has completed.

All configuration will be lost after downgrading the device. For FortiAnalyzer devices with hard drives installed, the hard drives will be formatted.

To re-initialize a FortiAnalyzer, use the following CLI commands via a console port connection:

```
execute reset all-settings
esecute format disk
```